UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/419,828 | 10/14/1999 | DON VAN DYKE | M-7084-US | 1859 |

24251 7590 07/07/2003

SKJERVEN MORRILL LLP
25 METRO DRIVE
SUITE 700
SAN JOSE, CA 95110

| EXAMINER |
|---|
| SMITHERS, MATTHEWS |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | 4 |

DATE MAILED: 07/07/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/419,828 | DYKE ET AL. | |
| | Examiner | Art Unit | |
| | Matthew B Smithers | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *14 October 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

## DETAILED ACTION

### *Information Disclosure Statement*

The information disclosure statement filed February 2, 2000 has been placed in the application file and the information referred to therein has been considered as to the merits.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent 6,028,939 granted to Yin.

Regarding claim 1, Yin meets the claimed limitations as follows:

"A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations."

see column 8, lines 15-17 and column 9, lines 21-30.

Regarding claim 2, Yin meets the claimed limitations as follows: "The computer system of Claim 1, wherein said computer system further comprises a register file providing operands to said arithmetic logic unit." see column 7, line 61 to column 8, line 37.

Regarding claim 3, Yin meets the claimed limitations as follows: "The computer system of Claim 2, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey." see column 5, line 54 to column 6, line 10 and column 7, line 61 to column 8, line 37.

Regarding claim 4, Yin meets the claimed limitations as follows: "The computer system of Claim 3, wherein said datum is 64 bits long and said subkey is 48 bits long." see column 5, lines 54-67.

Regarding claim 5, Yin meets the claimed limitations as follows: "The computer system of Claim 3, wherein said first and second portions each contain one-half number of bits of said datum." see column 5, lines 54-67.

Regarding claim 6, Yin meets the claimed limitations as follows: "The computer system of Claim 5, wherein each of said first and second portions is 32 bits long." see column 5, lines 54-67.

Regarding claim 7, Yin meets the claimed limitations as follows: "The computer system of Claim 3, wherein said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store

results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction." see column 5, line 54 to column 6, line 10 and column 7, line 61 to column 8, line 37.

Regarding claim 8, Yin meets the claimed limitations as follows:

"The computer system of Claim 7, wherein a bypass mechanism is provided in said register file such that said results are provided as input to said logic circuit without first being written back to said first, second and third registers." see column 5, line 54 to column 6, line 10 and column 7, line 61 to column 8, line 37.

Regarding claim 9, Yin meets the claimed limitations as follows:

"The computer system of Claim 8, wherein said register file and said bypass mechanism are shared by all instructions in said arithmetic logic unit." see column 5, line 54 to column 6, line 10 and column 7, line 61 to column 8, line 37.

Regarding claim 10, Yin meets the claimed limitations as follows:

"The computer system of Claim 1, further comprising a second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operating in parallel with said logic circuit." see column 5, lines 12-33.

Regarding claim 11, Yin meets the claimed limitations as follows:

"The computer system of Claim 1, wherein said logic circuit further comprises a circuit for selecting a subkey from a key." see column 5, line 67 to column 6, line 8.

Regarding claim 12, Yin meets the claimed limitations as follows:

"The computer system of Claim 11, wherein said key is 56 bits long." see column 5, line 67 to column 6, line 8.

Regarding claim 13, Yin meets the claimed limitations as follows:

"A process for performing encryption or decrryption under a Data Encryption Standard (DES) algorithm, comprising:

providing a logic circuit in an arithmetic logic unit;

and performing expansion permutation, S-box substitution and P-box permutation and associated XOR operations in said logic circuit." see column 8, lines 15-17 and column 9, lines 21-30.

Regarding claim 14, Yin meets the claimed limitations as follows:

"The process of Claim 13, further comprising performing shifting the output data of said logic circuit in a shift circuit in said arithmetic logic unit." see column 8, lines 38-58.

Regarding claim 15, Yin meets the claimed limitations as follows:

"The process of Claim 14, further comprising: storing operands in a register file; and providing said operands to said logic circuit." see column 7, line 61 to column 8, line 37.

Regarding claim 16, Yin meets the claimed limitations as follows:

"The process of Claim 15, further comprising:

storing a first portion of a datum for said encryption or decryption in first register in said register file;

storing a second portion of said datum for said encryption or decryption in second register in said register file; and

storing a subkey for said encryption or decryption in third register in said register file." see column 5, line 54 to column 6, line 10 and column 7, line 61 to column 8, line 37.

Regarding claim 17, Yin meets the claimed limitations as follows:

"The process of Claim 16, further comprising storing operands of an instruction executing one round of said DES algorithm in said first, second and third registers using said logic circuit and said shift circuit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction." see column 5, line 54 to column 6, line 10 and column 7, line 61 to column 8, line 37.

Regarding claim 18, Yin meets the claimed limitations as follows:

"The process of Claim 17, further comprising providing said results as input to said logic circuit without first being written back to said first, second and third registers." see column 5, line 54 to column 6, line 10 and column 7, line 61 to column 8, line 37.

Regarding claim 19, Yin meets the claimed limitations as follows:

The process of Claim 13, further comprising selecting a subkey from a key for said DES algorithm in a second logic circuit." see column 5, lines 12-33.

Regarding claim 20, Yin meets the claimed limitations as follows:

"The process of Claim 19, further comprising operating said second logic circuit in parallel with said logic circuit." see column 5, lines 12-33.

Regarding claim 21, Yin meets the claimed limitations as follows:

"The process of Claim 13, further comprising selecting a subkey from a key using a key select circuit in said logic circuit." see column 5, line 67 to column 6, line 8.

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Butter et al (5,381,480) discloses a system for translating encrypted block data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew B Smithers
Primary Examiner
Art Unit 2134

June 29, 2003